

PI

magazine
.com

professional investigator magazine

\$9.95

July/August 2024

THE CHECKLIST: A Simple,
Yet Essential Guide

APP-SOLUTE INSIGHT
Harnessing Everyday
Apps for Open Source
Intelligence

DEMOGRAPHICS for
the Private Investigator

STOICISM and the Art
of Private Investigation



CA SENATE BILL 553
Increased Business
Opportunities for
Security Consultants

Navigating the Depths
of WRONGFUL DEATH
INVESTIGATIONS

Don't Hold Back

The last of a four-part series
on the JonBenét Ramsey Case

DEPARTMENTS

MARKETING

22 FUTURE OF NETWORKING FOR PI'S: EMBRACING DIGITAL BUSINESS CARDS

By Catherine Flowers

BOOK SPOTLIGHT

24 UNRAVELED MYSTERIES: THE REALITY OF PRIVATE INVESTIGATION

By Bruce Nowlin and David Arndt

BACKGROUNDING

26 TESTING FOR THE OTHER DANGEROUS DRUG - ALCOHOL

By W. Barry Nixon

ALL THINGS SURVEILLANCE

28 BARE ESSENTIALS

By Eric De Van

BUSINESS

30 THE GROWING DEMAND FOR PRIVATE INVESTIGATORS IN AN ERA OF UNCERTAINTY

By Stephanie Savoy

INSURANCE

32 UNDERSTANDING KEY INSURANCE ENDORSEMENTS FOR PRIVATE INVESTIGATORS

By Kevin Whaley

TSCM

34 CORPORATE ESPIONAGE AND TRADE SECRET MISAPPROPRIATION: THE CASE OF APPIAN VS PEGASYSTEMS

By Tim O'Rourke

CYBERSLEUTHING

36 METADATA – IT MAY BE USEFUL BUT IT MAY BE UNRELIABLE

By Robert B. Fried

38 TO CRYPTO OR NOT TO CRYPTO, THAT IS THE QUESTION – SHOULD YOU CRYPTO?

By Christopher Salgado

BUSINESS-TAX

40 BUYING, RENTING OR LEASING

By Mark E. Battersby

IDENTITY THEFT

42 WHY IDENTITY THEFT CASES REQUIRE A SHIFT IN THINKING

By Carrie Kerskie

PI HISTORY

44 THE ELEPHANT IN THE ROOM

By Daniel Demers

SOCIAL MEDIA

46 VOIR DIRE: IS SOCIAL MEDIA THE NEW POLYGRAPH TEST?

By Kathy Doering

PROCESS SERVING

48 HEARD IT THROUGH THE GRAPEVINE

By Kevin Toal

PI PERSPECTIVES

52 MODERNIZING YOUR MARKETING APPROACH

By William F. Blake

NCISS LEGISLATIVE UPDATE

54 NEW U.S. DEPARTMENT OF LABOR RULE ON INDEPENDENT CONTRACTORS & IMPACTS ON THE INVESTIGATIVE PROFESSION

By Jim Zimmer and Edward Ajaeb

EXECUTIVE PROTECTION

58 THE POWER OF MAKING PREDICTIONS IN EXECUTIVE PROTECTION

By R. Preston Hocker

PI 101

60 THE IMPORTANCE OF BEING THOROUGH IN INVESTIGATIONS

By Malik Mubashshir

THE PI AND FUGITIVE RECOVERY

61 THE ART OF BODY LANGUAGE FOR THE PI

By Patrick L. Collis

INVESTIGATING INNOCENCE

62 THE ROLE OF THE DEFENSE INVESTIGATOR

By Kitty Hailey

IN EVERY ISSUE

PI Bookstore	25
Public Records Update	50
PI Conference Corner	64-65
Discover NALI.....	66-67
PI Resources.....	68-69
PI Seminars & Conference Calendar	71

METADATA

It May Be Useful But It May Be Unreliable

BY **ROBERT B. FRIED**

Perhaps you want to know who authored an 850-word document on a computer? Maybe you would like to know who last modified or printed the document? Metadata is defined as data about data. It can be useful to an investigator, providing key information that may be vital to an investigation.

Electronic evidence is fragile; and therefore, must be handled with care. Engaging a data collection specialist will ensure that the targeted data is collected in a forensically sound manner, whereas the integrity of the source data, including any associated metadata, is maintained. Simply copying and pasting a document from one storage volume to another may impact its metadata – specifically file created or last access dates and times. Other ways that metadata can be modified include updating values in a document’s properties via an operating system or utilizing a hex-editor.

It may be apparent by now that metadata is useful but it’s not necessarily reliable. Reviewing a document’s metadata alone may not reveal all the available information about a file. It’s important to consider how the document was created, who interacted with it, and where it was saved (if different from its current storage location). Metadata may only provide limited information about a document’s lifecycle. It’s important for the forensic examiner to have as much context as possible. Therefore, a forensic examiner may recommend obtaining a forensic image of the device or storage location where



the document is stored (remember, copies of a document may be stored in multiple locations, and different versions may exist). A forensic examiner can analyze a forensic image – specifically artifacts from the operating system or file system to learn more about a document. For example, a forensic examiner may be able to determine the series of actions and the dates and times associated with a computer user saving a document into a folder C:/Robert, and then subsequently copying it into another folder, C:/Fried.

Before taking any action on electronic evidence encountered during an investigation, it’s prudent to contact a data collection specialist. These individuals are trained to establish a proper chain of custody, preserve and collect evidence in a defensible and efficient manner – preventing claims of data spoliation – and ensuring its admissibility in a court of law. **PI**



25% Off Paperback Book & ECourse on Forensic Data Collections for PI Magazine Subscribers

**Coupon code: pimazine
www.forensicsbyfried.com**



Robert B. Fried has nearly 25 of experience performing data collections and forensic investigations of electronic evidence. He is the Senior Vice President and Global Head of Sandline Discovery’s Forensics and Investigations practice. Prior to joining Sandline, he was a Senior Director for Consilio’s Digital Forensics & Expert Services. Robert has also held senior-level positions for the data forensics practices at Huron Consulting Group and DOAR Litigation Consulting. Robert is a licensed

Professional Investigator in Michigan and is a licensed Private Investigator in New York. Previously, Robert was a Computer Crime Specialist at the National White Collar Crime Center (NW3C), where he developed and instructed computer forensic and investigative training courses for federal, state and local law enforcement agencies. Robert attained a BS and MS in Forensic Science from the University of New Haven. Additionally, Robert holds and actively maintains the following certifications: AccessData Certified Examiner (ACE), Certified Forensic Computer Examiner (CFCE), EnCase Certified Examiner (EnCE) and GLAC Certified Forensics Analyst (GCFA).